CLAIMS

Claims 1-28 (Cancelled)

29. (Currently Amended) A cryptographic feature enablement system comprising:

a processing unit;

a cryptographic chip including circuitry configured to perform encryption and decryption for each of a plurality of cryptographic systems wherein each of said plurality of cryptographic systems provides a different level of security;

a non-volatile read/write memory storing an encrypted token including encrypted initialization data for enabling said ~~circuitry configured~~ cryptographic chip to perform encryption and decryption for ~~a plurality of cryptographic systems to perform~~ one of said plurality of cryptographic systems in said cryptographic chip that provides a highest level of security in said cryptographic chip;

a bus connecting said processing unit to said non-volatile memory and said cryptographic chip to transmit data between said processing unit, said non-volatile memory, and said cryptographic chip; and

token decryption circuitry in said non-volatile memory to decrypt said encrypted initialization data in said encrypted token wherein said initialization data enables said circuitry in said cryptographic chip to perform encryption and decryption of data for said one of said plurality of cryptographic systems that provides said highest level of security.

30. (Previously Presented) The cryptographic feature enablement system of claim 29 wherein said at least one non-volatile read/write memory comprises FLASH memory.

31. (Previously Presented) The cryptographic feature enablement system of claim 29 wherein said non-volatile memory stores system specific information including a MAC address for said system.

32. (Previously Presented) The cryptographic feature enablement system of claim 31 wherein said MAC address is used to generate a private key.

33. (Currently Amended) A method for initializing cryptographic functionality in a system, the method comprising:

starting the boot process in a system;

using system-specific information of said system to generate a key;

decrypting an encrypted token stored in a non-volatile memory using said key wherein said encrypted token includes encrypted encryption initialization data;

determining whether said decrypted encryption initialization data from said encrypted token is useable for a cryptographic chip in said system; and

initializing said cryptographic chip to perform encryption and decryption in one of a plurality of cryptographic systems using said decrypted encryption initialization data responsive to a determination that said encryption initialization data is usable for said cryptographic chip wherein said cryptographic chip includes circuitry configured to encrypt and decrypt data in each of a plurality of cryptographic systems

each providing a different level of security and said one of said plurality of cryptographic systems provides a highest level of security.

34. (Previously Presented) The method of claim 33 where said system-specific information is said system's MAC address.

35. (Currently Amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine for initializing cryptographic functionality in a system, the method comprising:

starting the boot process in a system;

using system-specific information of said system to generate a key;

decrypting an encrypted token stored in a non-volatile memory using said key wherein said encrypted token includes encrypted encryption initialization data;

determining whether said decrypted encryption initialization data from said encrypted token is useable for a cryptographic chip in said system; and

initializing said cryptographic chip to perform encryption and decryption in one of a plurality of cryptographic systems using said decrypted encryption initialization data responsive to a determination that said encryption initialization data is usable for said cryptographic chip wherein each of said plurality of cryptographic system provides a different level of security and said one of said plurality of cryptographic systems provides a highest level of security.

36. (Previously Presented) The method of claim 35 where said system-specific information is said system's MAC address.

37. (Currently Amended) A system for initializing cryptographic functionality in a system, the system comprising:

means for starting the boot process in a system;

means for using system-specific information of said system to generate a key;

means for decrypting an encrypted token stored in a non-volatile memory using said key wherein said encrypted token includes encrypted encryption initialization data;

means for determining whether said decrypted encryption initialization data from said encrypted token is useable for a cryptographic chip in said system; and

means for initializing said cryptographic chip to perform encryption and decryption in one of a plurality of cryptographic systems using said decrypted encryption initialization data responsive to a determination that said encryption initialization data is usable for said cryptographic chip wherein said cryptographic chip provides said plurality of cryptographic systems wherein each of said plurality of cryptographic systems provides a different level of security and said one of said plurality of cryptographic systems provides a highest level of security.

38. (Previously Presented) The system of claim 37 where said system-specific information is said system's MAC address.

39. (Currently Amended) A method for installing cryptographic initialization data in a system for use during system booting, the method comprising:

identifying the system-specific information of said system;

generating a cryptographic key using said system-specific information;

using said cryptographic key to encrypt a token, wherein said token includes cryptographic initialization data applicable to a cryptographic chip in said system to cause said cryptographic chip to decrypt data in one of a plurality of encryption systems wherein said cryptographic chip provides a plurality of cryptographic systems wherein each of said plurality of cryptographic systems provides a different level of security and said one of said plurality of cryptographic systems provides a highest level of security; and,

writing said encrypted token in non-volatile memory of said system.

40. (Previously Presented) The method of claim 39 where said non-volatile memory is FLASH memory.

41. (Previously Presented) The method of claim 39 where said generation of at least one key further comprises generating a public key and a private key, and choosing said public key to encrypt said token and choosing said private key to use for decrypting said token.

42. (Previously Presented) The method of claim 39 where said system-specific information is said system's MAC address.

43. (Currently Amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by a machine for installing cryptographic initialization data in a system for use during system booting, the method comprising:

identifying the system-specific information of said system;

generating a cryptographic key using said system-specific information;

using said cryptographic key to encrypt a token, where said token comprises cryptographic initialization data ~~applicable to said system~~ for directing a cryptographic chip in said system to encrypt and decrypt data using one of a plurality of cryptographic systems said cryptographic chip is configured to perform and wherein each of said plurality of cryptographic systems perform a different level of security and said one of said plurality of cryptographic systems selected provides a highest level of security; and

writing said encrypted token in non-volatile memory in said system, where said non-volatile memory is configured to be accessible by a CPU in said system during system initialization.

44. (Previously Presented) The method of claim 43 where said non-volatile memory is FLASH memory.

45. (Previously Presented) The method of claim 43 where said generation of at least one key further comprises generating a public key and a private key, and choosing said public key to encrypt said token and choosing said private key to use for decrypting said token.

46. (Previously Presented) The method of claim 43 where said system-specific information is said system's MAC address.

47. (Currently Amended) A system for installing cryptographic initialization data in a system for use during system booting comprising:

means for identifying the system-specific information of said system;

means for generating a cryptographic key using said system-specific information;

means for using said cryptographic key of said at least one keys to encrypt a token, where said token comprises cryptographic initialization data ~~applicable to said system~~ for directing a cryptographic chip in said system to encrypt and decrypt data using one of a plurality of cryptographic systems said cryptographic chip is configured to perform and wherein each of said plurality of cryptographic systems perform a different level of security and said one of said plurality of cryptographic systems selected provides a highest level of security ; and[,]

means for writing said encrypted token in non-volatile memory in said system, where said non-volatile memory is configured to be accessible by a CPU in said system during system initialization.

48. (Previously Presented) The system of claim 47 where said non-volatile memory is FLASH memory.

49. (Previously Presented) The system of claim 47 where said means for generation of at least one key further comprises generating a public key and a private key, and choosing said public key to encrypt said token and choosing said private key to use for decrypting said token.

50. (Currently Amended) The system of claim 47 where said system-specific information is said system's MAC address.